

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization International Bureau



(43) International Publication Date
3 March 2005 (03.03.2005)

PCT

(10) International Publication Number
WO 2005/020541 A1

(51) International Patent Classification⁷: **H04L 29/06, G06F 1/00**

(21) International Application Number: **PCT/US2004/002407**

(22) International Filing Date: 27 January 2004 (27.01.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data: 60/494,836 13 August 2003 (13.08.2003) US

(71) Applicant (for all designated States except US): THOMSON LICENSING S.A. [FR/FR]; 46, Quai A. LeGallo, 92648 Boulogne Cedex (FR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): ZHANG, Junbiao [CN/US]; 20 Jenna Drive, Bridgewater, NJ 08807 (US). LI, Jun [CN/US]; 26 Orchid Drive, Plainsboro, NJ 08536

(74) Agents: TRIPOLI, Joseph, S. et al.; 2 Independence Way, Princeton, NJ 08540 (US).

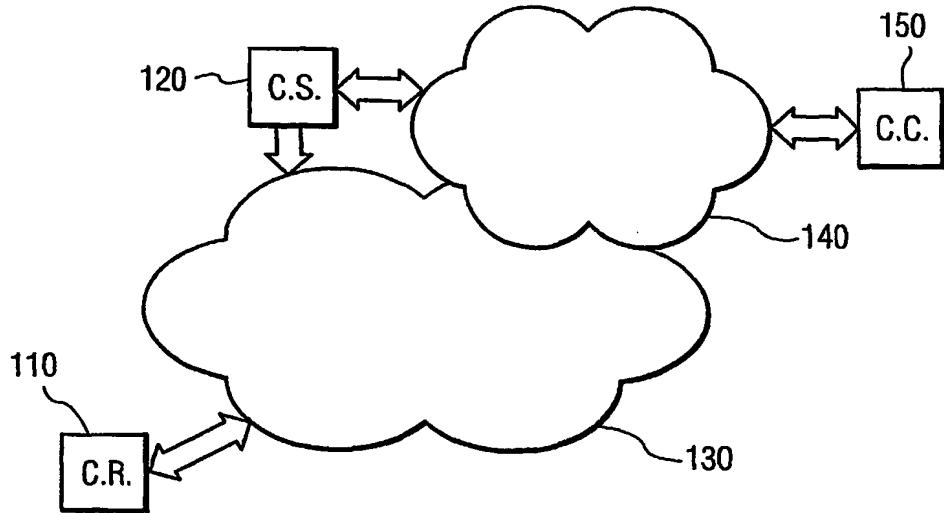
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,

[Continued on next page]

(54) Title: METHOD AND DEVICE FOR SECURING CONTENT DELIVERY OVER A COMMUNICATION NETWORK VIA CONTENT KEYS

100



(57) Abstract: A method for descrambling secure content received over a network is disclosed. The method is operable at a receiving device (150) located at a remote site in communication with a network (140) for receiving a first information item scrambled using an encrypting key (Pu) known by the remote site, descrambling the first information item using a corresponding decrypting key, wherein the information item includes an access code (CAC) and a content key (Kc), receiving a second information item, scrambled using the content key after a server, (120) hosting the second information item verifies the access code (CAC) and descrambling the second information item using the content key (Kc).

WO 2005/020541 A1



TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *with international search report*